EXISTENCE OF RATIONAL POINTS ON SMOOTH PROJECTIVE VARIETIES

BJORN POONEN

to Jean-Louis Colliot-Thélène on his 60^{th} birthday

Abstract. Fix a number field k. We prove that if there is an algorithm for deciding whether a smooth projective geometrically integral k-variety has a k-point, then there is an algorithm for deciding whether an arbitrary k-variety has a k-point and also an algorithm for computing $X(k)$ for any k-variety X for which $X(k)$ is finite. The proof involves the construction of a one-parameter algebraic family of Châtelet surfaces such that exactly one of the surfaces fails to have a k-point.

1. Statement of results

A variety over a field k is a separated scheme of finite type over k. We will consider algorithms (Turing machines) accepting as input k-varieties where k is a number field. Each such variety may be presented by a finite number of affine open patches together with gluing data, so it admits a finite description suitable for input into a Turing machine. We do not require algorithms to run in polynomial time or any other specified time, but they must terminate with an answer for each allowable input.

Theorem 1.1. *Fix a number field k. Suppose that there exists an algorithm for deciding whether a regular projective geometrically integral k-variety has a k-point. Then*

(i) *There is an algorithm for deciding whether an arbitrary k-variety has a k-point.*
(ii) *There is an algorithm for computing $X(k)$ for any k-variety X for which $X(k)$ is finite.*

Remark 1.2.

(a) For a field k of characteristic 0, a k-variety is regular if and only if it is smooth over k. Nevertheless, we have two reasons for sometimes using the adjective "regular":
- In some situations, for instance when speaking of families of varieties, it helps to distinguish the absolute notion (regular) from the relative notion (smooth).
- In Section 10, we say what can be said about the analogue for global function fields.

Date: December 11, 2007.
2000 *Mathematics Subject Classification.* Primary 14G05; Secondary 11G35, 11U05, 14G25, 14J20.
Key words and phrases. Brauer-Manin obstruction, Hasse principle, Châtelet surface, conic bundle, rational points.
This research was supported by NSF grant DMS-0301280.

(b) For regular proper integral k-varieties, the property of having a k-point is a birational invariant, equivalent to the existence of a (not necessarily rank 1) valuation v on the function field such that v is trivial on k and k maps isomorphically to the residue field: this follows from [Nis55] and also is close to [Lan54, Theorem 3]; see also [CTCS80, Lemme 3.1.1]. Thus one might wonder whether the decision problem is easier for regular projective geometrically integral varieties than for arbitrary ones. But Theorem 1.1(i) says that in fact the two problems are equivalent.

(c) For $k = \mathbb{Q}$, Theorem 1.1(i) was more or less known: it is easily deduced from a result of R. Robinson [Smo91, §II.7] that the problem of deciding the existence of a rational zero of a polynomial over $\mathbb{Q}$ is equivalent to the problem of deciding the existence of a nontrivial rational zero of a *homogeneous* polynomial over $\mathbb{Q}$. Robinson's argument generalizes easily to number fields with a real place.

(d) Theorem 1.1 becomes virtually trivial if the word "projective" is changed to "affine". On the other hand, there are related statements for affine varieties that are nontrivial: for instance, if there is an algorithm for deciding whether any irreducible affine plane curve of geometric genus at least 2 has a rational point, then there is algorithm for determining the set of rational points on any such curve [Kim03].

(e) By restriction of scalars, if we have an algorithm for deciding whether a regular projective geometrically integral variety over $\mathbb{Q}$ has a rational point, then we have an analogous algorithm over any number field.

(f) Remark 7.2 will imply that to have algorithms in (i) and (ii) of Theorem 1.1 for *curves*, it would suffice to be able to decide the existence of rational points on regular projective geometrically integral 3-*folds*. (If over $\mathbb{Q}$ one uses Robinson's reduction instead, one would need an algorithm for 9-folds!)

Theorem 1.1 will be deduced in Section 9 from the following:

Theorem 1.3. *Let X be a projective variety over a number field k. Let $U \subseteq X$ be an open subvariety. Then there exists a regular projective variety Y and a morphism $\pi\colon Y \to X$ such that $\pi(Y(k)) = U(k)$. Moreover, there exists an algorithm for constructing (Y, π) given (k, X, U).*

The key special case, from which all others will be derived, is the case where $U = \mathbb{A}^1$ and $X = \mathbb{P}^1$. In this case we can arrange also for $\pi^{-1}(t)$ to be smooth and geometrically integral for all $t \in \mathbb{P}^1(k)$: see Proposition 6.2. Thus we will have a family of smooth projective geometrically integral varieties in which every rational fiber but one has a rational point, an extreme example of geometry *not* controlling arithmetic!

Remark 1.4. Theorem 1.3 fails for many fields k that are not number fields, even for those that have a complicated arithmetic. Proposition 6.3 implies that it fails for the function field of any variety over $\mathbb{C}$, for instance.

2. Notation

Let k be a number field. Let $\mathcal{O}_k$ be the ring of integers in k. If v is a place of k, let k_v be the completion of k at v. If v is nonarchimedean, let $\mathbb{F}_v$ be the residue field; call v odd if $\#\mathbb{F}_v$ is odd. If $a \in \mathcal{O}_k$ generates a prime ideal, let v_a be the associated valuation, and let $\mathbb{F}_a = \mathbb{F}_{v_a}$. For $a \in k$, let $a \gg 0$ mean that a is totally positive, i.e., positive for every real embedding of k.

3. Conic bundles

A conic over k is the zero locus in $\mathbb{P}^2 = \operatorname{Proj} k[x_0, x_1, x_2]$ of a nonzero degree-2 homogeneous polynomial in $k[x_0, x_1, x_2]$. A conic bundle C over a k-scheme B is the zero locus in $\mathbb{P}\mathcal{E}$ of a nowhere vanishing section s of $\operatorname{Sym}^2 \mathcal{E}$, where $\mathcal{E}$ is some rank-3 vector sheaf on B. We will consider only the special case where $\mathcal{E} = \mathcal{L}_0 \oplus \mathcal{L}_1 \oplus \mathcal{L}_2$ for some line sheaves $\mathcal{L}_i$ and $s = s_0 + s_1 + s_2$ where $s_i \in \Gamma(B, \mathcal{L}_i^{\otimes 2})$; we then call $C \to B$ a diagonal conic bundle.

Remark 3.1. If B is a smooth curve over k and $\sum_{i=0}^{2} \operatorname{ord}_P(s_i) \leq 1$ for every $P \in B$, then the total space C is smooth over k.

4. Châtelet surfaces

Fix $\alpha \in k^\times$ and $P(x) \in k[x]$ of degree at most 4. Let V_0 be the affine surface in $\mathbb{A}^3$ given by $y^2 - \alpha z^2 = P(x)$. We want a smooth projective model V of V_0. Define $\tilde{P}(w, x) := w^4 P(x/w)$; view $\tilde{P}$ as a section of $\mathcal{O}(4)$ on $\mathbb{P}^1 := \operatorname{Proj} k[w, x]$. The construction of Section 3 with $B = \mathbb{P}^1$, $\mathcal{L}_0 = \mathcal{L}_1 = \mathcal{O}$, $\mathcal{L}_2 = \mathcal{O}(2)$, $s_0 := 1$, $s_1 := -\alpha$, and $s_2 := -\tilde{P}$ gives a diagonal conic bundle $V \to \mathbb{P}^1$ containing V_0 as an affine open subvariety. Since $V \to \mathbb{P}^1$ is projective, V is projective over k too. If $P(x)$ is not identically 0, then V is geometrically integral. If $P(x)$ is separable and of degree 3 or 4, then $\tilde{P}(w, x)$ is separable and V is smooth over k by Remark 3.1; in this case V is called the Châtelet surface given by $y^2 - \alpha z^2 = P(x)$.

Iskovskikh [Isk71] showed that the Châtelet surface over $\mathbb{Q}$ given by

$$y^2 + z^2 = (x^2 - 2)(3 - x^2)$$

violated the Hasse principle. Several years later it was shown that this violation could be explained by the Brauer-Manin obstruction, and that more generally, any Châtelet surface over a number field given by $y^2 - az^2 = f(x)g(x)$ with f and g distinct irreducible quadratic polynomials satisfies the Hasse principle if and only if there is no Brauer-Manin obstruction [CTCS80, Theorem B]. Finally, the two-part paper [CTSSD87, CTSSD87b] generalized this to all Châtelet surfaces over number fields.

Proposition 4.1. *Over every number field k, there exists a Châtelet surface V that violates the Hasse principle.*

The rest of this section is devoted to the proof of Proposition 4.1, so a reader interested in only the case $k = \mathbb{Q}$ may accept the Iskovskikh example and proceed to Section 5. We generalize the argument presented in [Sko01, p. 145].

By the Chebotarev density theorem, we can find $b \in \mathcal{O}_k$ generating a prime ideal such that $b \gg 0$ and $b \equiv 1 \pmod{8\mathcal{O}_k}$. Similarly we find $a \in \mathcal{O}_k$ generating a prime ideal such that $a \gg 0$ and $a \equiv 1 \pmod{8\mathcal{O}_k}$ and a is a not a square modulo b. We may assume that $\#\mathbb{F}_a, \#\mathbb{F}_b > 5$. Fix $c \in \mathcal{O}_k$ such that $b | (ac + 1)$.

Let $(x, y)_v \in \{\pm 1\}$ be the v-adic Hilbert symbol. Define $(x, y)_b := (x, y)_{v_b}$. We will need the following Hilbert symbol calculations later:

Lemma 4.2. *We have*

(i) $(-1, a)_v = 1$ *for all* v.
(ii) $(-1, b)_v = 1$ *for all* v.
(iii) $(ab, a)_b = -1$.
(iv) $(ab, c)_b = -1$.

Proof.

(i) For v archimedean or 2-adic, it follows from $a \in k_v^{\times 2}$. For all other v except v_a, it follows from $v(-1) = v(a) = 0$. For $v = v_a$, it follows from the product formula.

(ii) The proof is the same as that of (i).

(iii) By (i), $(ab, a)_b = (-ab, a)_b = (-a, a)_b (b, a)_b = 1 \cdot (b, a)_b = -1$, by choice of a.

(iv) Since $b|(ac+1)$, we have $(ab, ac)_b = (ab, -1)_b = (a, -1)_b (b, -1)_b = 1$ by (i) and (ii). Divide by (iii) to get $(ab, c)_b = -1$. □

Let V be the Châtelet surface given by

$$y^2 - abz^2 = (x^2 + c)(ax^2 + ac + 1). \tag{1}$$

(The quadratic factors on the right are separable and generate the unit ideal of $k[x]$, so V is smooth over k.)

Lemma 4.3. *The variety V has a k_v-point for every place v of k.*

Proof. Suppose that v is archimedean or 2-adic. Then $ab \in k_v^{\times 2}$, so V has a k_v-point.

Suppose that v is odd and $v \notin \{v_a, v_b\}$. Choose $x \in k$ with $v(x) < 0$. Then the right hand side of (1) has even valuation and is hence a norm for the unramified extension $k_v(\sqrt{ab})/k_v$. So V has a k_v-point.

Suppose that $v = v_b$. The number of solutions to $y^2 = a(x^2 + c)$ over $\mathbb{F}_b$ with $x^2 + c \neq 0$ and $x \neq 0$ is at least $(\#\mathbb{F}_b + 1) - 2 - 2 - 2 > 0$. Choose $x \in \mathcal{O}_k$ reducing to such a solution. The right hand side of (1) is congruent modulo b to $(x^2 + c)(ax^2)$, so by Hensel's lemma it is in $k_v^{\times 2}$. Thus V has a k_v-point.

Suppose that $v = v_a$. The same argument as in the previous paragraph shows that we may choose $x \in \mathcal{O}_k$ such that $x^2 + c \in k_v^{\times 2}$. The other factor $ax^2 + ac + 1$ is 1 mod a, hence in $k_v^{\times 2}$. Therefore the right hand side of (1) is in $k_v^{\times 2}$, so V has a k_v-point. □

Let $\kappa(V)$ be the function field of V. Let $A \in \operatorname{Br} \kappa(V)$ be the class of the quaternion algebra $(ab, x^2 + c)$. Then A equals the class of $(ab, ax^2 + ac + 1)$ and of $(ab, 1 + c/x^2)$, so $A \in \operatorname{Br} V$. We will show that A gives a Brauer-Manin obstruction to the Hasse principle. For $P_v \in V(k_v)$, let $A(P_v) \in \operatorname{Br} k_v$ be the evaluation of A at P_v. Let $\operatorname{inv}_v \colon \operatorname{Br} k_v \hookrightarrow \mathbb{Q}/\mathbb{Z}$ be the usual invariant map.

Lemma 4.4. *For any $P_v \in V(k_v)$,*

$$\operatorname{inv}_v(A(P_v)) = \begin{cases} 0, & \text{if } v \neq v_b, \\ 1/2 & \text{if } v = v_b. \end{cases}$$

Proof. By continuity, we may assume $P_v \in V_0(k_v)$. Suppose that v is archimedean or 2-adic. Then $ab \in k_v^{\times}$, so A maps to 0 in $\operatorname{Br} k_v(V)$. Hence $\operatorname{inv}_v(A(P_v)) = 0$.

Suppose that v is odd and $v \notin \{v_a, v_b\}$. If $v(x) < 0$ at P_v, then $v(x^2 + c)$ is even, so $\operatorname{inv}_v(A(P_v)) = 0$. If $v(x) \geq 0$, then either $x^2 + c$ or $ax^2 + ac + 1$ is a v-adic unit, so using an appropriate description of A shows that $\operatorname{inv}_v(A(P_v)) = 0$.

Suppose that $v = v_a$. If $v(x) < 0$ at P_v, then $x^2 + c \in k_v^{\times 2}$, so $\operatorname{inv}_v(A(P_v)) = 0$. If $v(x) \geq 0$, then $ax^2 + ac + 1$ is 1 mod a so it is in $k_v^{\times 2}$, and again $\operatorname{inv}_v(A(P_v)) = 0$.

Finally, suppose that $v = v_b$. If $v(x) \leq 0$, then $b|(ac+1)$ implies $(ab, ax^2 + ac + 1)_b = (ab, ax^2)_b = (ab, a)_b = -1$ by Lemma 4.2(iii). If $v(x) > 0$, then $(ab, x^2 + c)_b = (ab, c)_b = -1$ by Lemma 4.2(iv). In either case, $\operatorname{inv}_v(A(P_v)) = 1/2$. □

Lemma 4.4 implies that V has no k-point. This completes the proof of Proposition 4.1.

5. Châtelet surface bundles

By a Châtelet surface bundle over $\mathbb{P}^1$ we mean a flat proper morphism $\mathcal{V} \to \mathbb{P}^1$ such that the generic fiber is a Châtelet surface. For $t \in \mathbb{P}^1(k)$, we let $\mathcal{V}_t$ be the fiber above t.

We retain the notation of Section 4. Let $\tilde{P}_0(w,x) \in k[w,x]$ be the homogeneous form of degree-4 obtained by homogenizing the right hand side of (1). Let $\tilde{P}_\infty(w,x)$ be any irreducible degree-4 form in $k[w,x]$. Thus $\tilde{P}_0$ and $\tilde{P}_\infty$ are linearly independent.

Let $\mathcal{V}$ be the diagonal conic bundle over $\mathbb{P}^1 \times \mathbb{P}^1 := \operatorname{Proj} k[u,v] \times \operatorname{Proj} k[w,x]$ obtained by taking $\mathcal{L}_0 = \mathcal{L}_1 := \mathcal{O}$, $\mathcal{L}_2 := \mathcal{O}(1,2)$, $s_0 := 1$, $s_1 := -ab$, and $s_2 := -(u^2\tilde{P}_\infty + v^2\tilde{P}_0)$. Composing $\mathcal{V} \to \mathbb{P}^1 \times \mathbb{P}^1$ with the first projection $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ lets us view $\mathcal{V}$ as a Châtelet surface bundle over $\mathbb{P}^1 = \operatorname{Proj} k[u,v]$ with projective geometrically integral fibers. If $u, v \in k$ are not both 0, the fiber above $(u:v) \in \mathbb{P}^1(k)$ is the Châtelet surface given by

$$y^2 - abz^2 = u^2\tilde{P}_\infty(1,x) + v^2\tilde{P}_0(1,x),$$

if smooth over k. In particular, the fiber $\mathcal{V}_{(0:1)}$ is isomorphic to V.

Lemma 5.1. *The set of specializations $(u:v) \in \mathbb{P}^1(k)$ such that $u^2\tilde{P}_\infty + v^2\tilde{P}_0 \in k[w,x]$ is reducible (for any or all choices of $(u,v) \in k^2 - \{(0,0)\}$ representing $(u:v)$) is a thin set in the sense of* [Ser97, §9.1].

Proof. We may assume $u = 1$. The degree-4 form $\tilde{P}_\infty + v^2\tilde{P}_0$ over $k(v)$ is irreducible since it has an irreducible specialization, namely $\tilde{P}_\infty$. Apply [Ser97, §9.2, Proposition 1]. $\square$

Lemma 5.2. *There exists a finite set S of non-complex places of k and a neighborhood N_v of $(0:1)$ in $\mathbb{P}^1(k_v)$ for each $v \in S$ such that for $t \in \mathbb{P}^1(k)$ belonging to N_v for each $v \in S$, the fiber $\mathcal{V}_t$ has a k_v-point for* every *v.*

Proof. This is an application of the "fibration method", which has been used previously in various places (e.g., [CTSSD87], [CT98, 2.1], [CTP00, Lemma 3.1]). Since all geometric fibers of the k-morphism $\mathcal{V} \to \mathbb{P}^1$ are integral, the same is true for a model over some ring $\mathcal{O}_{k,S}$ of S-integers. By adding finitely many v to S, we can arrange that for nonarchimedean $v \notin S$ the residue field $\mathbb{F}_v$ is large enough that every $\mathbb{F}_v$-fiber has a smooth $\mathbb{F}_v$-point by the Weil conjectures; then by Hensel's lemma any k_v-fiber has a k_v-point. Include the real places in S, and exclude the complex places since for complex v the existence of k_v-points on fibers is automatic. For $v \in S$, since the fiber above $(0:1)$ has a k_v-point, and since $\mathcal{V} \to \mathbb{P}^1$ is smooth above $(0:1)$, the implicit function theorem implies that the image of $\mathcal{V}(k_v) \to \mathbb{P}^1(k_v)$ contains a v-adic neighborhood N_v of $(0:1)$ in $\mathbb{P}^1(k_v)$. $\square$

6. Base change

The following lemma combines the idea of [CTP00, Lemma 3.3] with some new ideas.

Lemma 6.1. *Let $P \in \mathbb{P}^1(k)$. Let S be a finite set of non-complex places of k. For each $v \in S$, let N_v be a neighborhood of P in $\mathbb{P}^1(k_v)$. Let T be a thin subset of $\mathbb{P}^1(k)$ containing P. Then there exists a k-morphism $\gamma\colon \mathbb{P}^1 \to \mathbb{P}^1$ such that both of the following hold:*

(1) *$\gamma(\mathbb{P}^1(k_v)) \subseteq N_v$ for each $v \in S$.*
(2) *$\gamma^{-1}(T) \cap \mathbb{P}^1(k)$ consists of a single point Q with $\gamma(Q) = P$.*

Proof. We will construct γ as a composition. But we present the argument as a series of reductions, each step of which involves taking the inverse image of all the data under some $\beta\colon \mathbb{P}^1 \to \mathbb{P}^1$ and replacing P by some $P' \in \beta^{-1}(P) \cap \mathbb{P}^1(k)$.

By definition of thin, there exist finitely many regular projective geometrically integral curves C_i and morphisms $\nu_i\colon C_i \to \mathbb{P}^1$ of degree greater than 1 such that $T \subseteq \bigcup \nu_i(C_i(k))$. Choose $Q \in \mathbb{P}^1(k)$ not equal to a branch point of any ν_i. Let $\beta\colon \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism of some large degree n such that β is totally ramified above P and Q and unramified elsewhere. Define $\nu_i'\colon C_i' \to \mathbb{P}^1$ to make the diagram

$$\begin{tikzcd} C_i' \arrow[r] \arrow[d, "\nu_i'"'] & C_i \arrow[d, "\nu_i"] \\ \mathbb{P}^1 \arrow[r, "\beta"] & \mathbb{P}^1 \end{tikzcd}$$

cartesian. Since $C_i' \to C_i$ is totally ramified above $\nu_i^{-1}(Q)$, each C_i' is geometrically integral. The morphism $C_i \to \mathbb{P}^1$ must have a branch point $R \in \mathbb{P}^1(\overline{k})$ other than P, and by choice of Q we have $R \neq Q$, so $\beta^{-1}(R)$ gives n branch points of $\nu_i'\colon C_i' \to \mathbb{P}^1$. On the other hand, $\deg \nu_i' = \deg \nu_i$, so if n is sufficiently large, the Hurwitz formula implies that the normalization of C_i' has genus greater than 1. By Faltings' theorem [Fal83], $C_i'(k)$ is finite. We have $\beta^{-1}(T) \subseteq \bigcup \nu_i'(C_i'(k))$, so $\beta^{-1}(T)$ is finite. By pulling all the data back under β, we reduce to the case where T is finite.

We may assume that $P = 0 \in \mathbb{P}^1(k)$ with respect to some coordinate. Then the rational function $t \mapsto 1/(t^2+m)$ maps ∞ to 0 and maps $\mathbb{P}^1(\mathbb{R})$ into N_v for each real v if $m \in \mathbb{Z}_{>0}$ is chosen large enough. Pulling all the data back under the corresponding automorphism of $\mathbb{P}^1$, we reduce to the case where S contains no archimedean places. Similarly, for each nonarchimedean $v \in S$, let $q = \#\mathbb{F}_v$, choose a rational function g mapping $\{0,1,\infty\}$ to P, and pull back everything under the rational function $g(t^m)$ where $m = q^r(q-1)$ for some large r; this lets us replace S by $S - \{v\}$. Eventually we reduce to the case in which $S = \emptyset$.

For a suitable choice of coordinate, P is the point $0 \in \mathbb{P}^1(k)$, and $\infty \notin T$. Choose $c \in k^\times$ such that the images of c and $T - \{0\}$ in $k^\times/k^{\times 2}$ do not meet. Let $\gamma\colon \mathbb{P}^1 \to \mathbb{P}^1$ be given by the rational function ct^2. Then $\gamma^{-1}(T) \cap \mathbb{P}^1(k)$ consists of the single point 0. ☐

Proposition 6.2. *There exists a Châtelet surface bundle $\mu\colon \mathcal{W} \to \mathbb{P}^1$ over k such that*

(i) *μ is smooth over $\mathbb{P}^1(k)$, and*
(ii) *$\mu(\mathcal{W}(k)) = \mathbb{A}^1(k)$.*

Proof. Obtain $\gamma\colon \mathbb{P}^1 \to \mathbb{P}^1$ from Lemma 6.1 with $P = (0:1)$, with S and N_v as in Lemma 5.2, with T the thin set of Lemma 5.1; note that T contains the finitely many $t \in \mathbb{P}^1(k)$ above which $\mathcal{V} \to \mathbb{P}^1$ is not smooth. We may assume that the Q in Lemma 6.1 is ∞. Define $\mathcal{W}$ as the fiber product

$$\begin{tikzcd} \mathcal{W} \arrow[r] \arrow[d, "\mu"'] & \mathcal{V} \arrow[d] \\ \mathbb{P}^1 \arrow[r, "\gamma"] & \mathbb{P}^1. \end{tikzcd}$$

Then μ is smooth above $\mathbb{P}^1(k)$, and for every $t \in \mathbb{P}^1(k)$ the fiber $\mathcal{W}_t$ has a k_v-point for every v. If $t \in \mathbb{A}^1(k)$, then $\gamma(t) \notin T$, so $\mathcal{W}_t$ is a Châtelet surface defined by an irreducible degree-4

polynomial, so by [CTSSD87, Theorem B(i)(b)] $\mathcal{W}_t$ satisfies the Hasse principle; thus $\mathcal{W}_t$ has a k-point. But if $t = \infty$, then $\mathcal{W}_t$ is isomorphic to $\mathcal{V}_{(0:1)} \simeq V$, which has no k-point. $\square$

The following proposition will not be needed elsewhere. Its role is only to illustrate that Theorem 1.3 and Proposition 6.2 depend subtly upon properties of k: for instance, they are not true over all fields of cohomological dimension 2.

Proposition 6.3. *Let k_0 be an uncountable algebraically closed field, and let k be a field extension of k_0 generated by a set S of cardinality less than $\#k_0$. Then there is no morphism $\pi\colon \mathcal{W} \to \mathbb{P}^1$ of projective k-varieties such that $\pi(\mathcal{W}(k)) = \mathbb{A}^1(k)$.*

Proof. Suppose that $\pi(\mathcal{W}(k)) = \mathbb{A}^1(k)$. Fix a projective embedding $\mathcal{W} \hookrightarrow \mathbb{P}^n_k$. For each k_0-subspace L of k spanned by finitely many finite products of elements of S, let $\mathcal{W}(L)$ be the set of points in $\mathcal{W}(k) \subseteq \mathbb{P}^n(k)$ represented by an $(n+1)$-tuple of elements of L, not all zero. The set of points in $\mathbb{P}^1(k_0) \subseteq \mathbb{P}^1(k)$ in the image of $\mathcal{W}(L) \to \mathbb{P}^1(k)$ is a Zariski closed subset of $\mathbb{P}^1(k_0)$ not containing ∞, and hence finite. Taking the union over all L, we find that the set of points in $\mathbb{P}^1(k_0)$ in the image of $\mathcal{W}(k) \to \mathbb{P}^1(k)$ has cardinality at most $\max\{\#S, \aleph_0\}$, which is less than $\#k_0$. In particular, $\pi(\mathcal{W}(k))$ cannot be a cofinite subset of $\mathbb{P}^1(k)$. $\square$

7. Reductions

Lemma 7.1. *There exists a projective k-variety Z and a morphism $\eta\colon Z \to \mathbb{P}^n$ such that $\eta(Z(k)) = \mathbb{A}^n(k)$ and η is smooth above $\mathbb{A}^n(k)$.*

Proof. Start with the birational map $(\mathbb{P}^1)^n \dashrightarrow \mathbb{P}^n$ given by the isomorphism $(\mathbb{A}^1)^n \to \mathbb{A}^n$. Resolve the indeterminacy; i.e., find a projective k-variety J and a birational morphism $J \to (\mathbb{P}^1)^n$ whose composition with $(\mathbb{P}^1)^n \dashrightarrow \mathbb{P}^n$ extends to a morphism $J \to \mathbb{P}^n$ that is an isomorphism above $\mathbb{A}^n$. Define Z to make a cartesian square

$$\begin{tikzcd} Z \arrow[r] \arrow[d] & \mathcal{W}^n \arrow[d, "\mu^n"] & \\ J \arrow[r] \arrow[rr, bend right] & (\mathbb{P}^1)^n \arrow[r, dashed] & \mathbb{P}^n \end{tikzcd}$$

where $\mathcal{W} \xrightarrow{\mu} \mathbb{P}^1$ is as in Proposition 6.2. Let η be the composition $Z \to J \to \mathbb{P}^n$.

By construction of $\mathcal{W}$, we have $\mu^n(\mathcal{W}^n(k)) = (\mathbb{A}^1)^n(k)$, so the image of $Z(k) \to J(k)$ is contained in the copy of $\mathbb{A}^n$ in J. Therefore $\eta(Z(k)) \subseteq \mathbb{A}^n(k)$.

On the other hand, if $t \in \mathbb{A}^n(k)$, then $J \to (\mathbb{P}^1)^n$ is a local isomorphism above t, and $\mathcal{W}^n \to (\mathbb{P}^1)^n$ is smooth above t, so $Z \to J$ is smooth above t, and the fiber $\eta^{-1}(t)$ is isomorphic to the corresponding fiber of $\mathcal{W}^n \to (\mathbb{P}^1)^n$ so it has a k-point. Thus $\eta(Z(k)) = \mathbb{A}^n(k)$. $\square$

Proof of existence in Theorem 1.3. We use induction on $\dim X$. We may assume that X is integral and that $X(k)$ is Zariski dense in X; then X is generically smooth, and the non-smooth locus X_{sing} is of lower dimension. Let $U_{\text{sing}} = U \cap X_{\text{sing}}$. The inductive hypothesis gives $\pi_1\colon Y_1 \to X_{\text{sing}}$ such that $\pi_1(Y_1(k)) = U_{\text{sing}}(k)$. If we prove the conclusion for $U - U_{\text{sing}} \subseteq X$, i.e., if we find $\pi_2\colon Y_2 \to X$ such that $\pi_2(Y_2(k)) = (U - U_{\text{sing}})(k)$, then the disjoint union $Y_1 \coprod Y_2$ serves as a Y for $U \subseteq X$. Thus we reduce to the case where U is smooth over k.

If U is a finite union of open subvarieties U_i, then it suffices to prove the conclusion for each $U_i \subseteq X$ and take the disjoint union of the resulting Y's. In particular, we may reduce

to the case where $U = X - D$ for some very ample effective divisor $D \subseteq X$. In other words, we may assume that $X \subseteq \mathbb{P}^n$ and $U = X \cap \mathbb{A}^n$.

Let $Z \to \mathbb{P}^n$ be as in Lemma 7.1. Define Y_0 to make a cartesian diagram

$$\begin{tikzcd}
Y \arrow[dr] \arrow[ddr, dotted, bend right, "\pi"'] & & \\
& Y_0 \arrow[r] \arrow[d] & Z \arrow[d, "\eta"] \\
& X \arrow[r, hook] & \mathbb{P}^n \\
U \arrow[ur, hook] \arrow[r, hook] & \mathbb{A}^n \arrow[ur, hook] &
\end{tikzcd}$$

and let $Y \to Y_0$ be a resolution of singularities that is an isomorphism above the smooth locus of Y_0, so Y is a regular projective variety. Let π be the composition $Y \to Y_0 \to X$.

Suppose that $t \in U(k)$. Then $Z \to \mathbb{P}^n$ is smooth above t, by choice of Z. So $Y_0 \to X$ is smooth above t. Moreover, $U \to \operatorname{Spec} k$ is smooth, so $Y_0 \to \operatorname{Spec} k$ is smooth above t. Therefore $Y \to Y_0$ is a local isomorphism above t. Thus $\pi^{-1}(t) \simeq \eta^{-1}(t)$, and the latter has a k-point.

On the other hand, if $t \in X(k) - U(k)$, then $\pi^{-1}(t)$ cannot have a k-point, since such a k-point would map to a k-point of Z lying over $t \in \mathbb{P}^n(k) - \mathbb{A}^n(k)$, contradicting the choice of Z.

Thus $\pi(Y(k)) = U(k)$. $\square$

Remark 7.2. In the special case where X is a regular projective curve and U is an affine open subvariety of X, the reductions may be simplified greatly. Namely, using the Riemann-Roch theorem, construct a morphism $f\colon X \to \mathbb{P}^1$ such that $f^{-1}(\infty) = X - U$; now define Y_0 to make a cartesian diagram

$$\begin{tikzcd}
Y \arrow[dr] \arrow[ddr, dotted, bend right, "\pi"'] & & \\
& Y_0 \arrow[r] \arrow[d] & \mathcal{W} \arrow[d, "\mu"] \\
& X \arrow[r, "f"] & \mathbb{P}^1
\end{tikzcd}$$

and let Y be a resolution of singularities of Y_0.

8. Effectivity

The construction of Y in Theorem 1.3 as given is not effective, because it used Faltings' theorem. More specifically, in the proof of Lemma 6.1 we know that $C_i'(k)$ is finite but might not know what it is, so when we reach the last paragraph of the proof, we might not know what the finite set T is, and hence we have no algorithm for computing a good c, where good means that the images of c and $T - \{0\}$ in $k^\times / k^{\times 2}$ do not meet.

Existence of an algorithm for Theorem 1.3. Let F be the (finite) set of $t \in \mathbb{P}^1(k)$ such that $\mathcal{V}_t$ is not smooth. Suppose that instead of requiring that c be good, we require only the

effectively checkable condition that the images of c and F in $k^\times/k^{\times 2}$ do not meet. Then the proof of existence in Theorem 1.3 still yields a regular projective variety Y_c and a morphism $\pi_c\colon Y_c \to X$, but it might not have the desired property $\pi_c(Y_c(k)) = U(k)$. Indeed, in the proof of Proposition 6.2, some of the Châtelet surfaces $\mathcal{W}_t$ other than $\mathcal{W}_\infty$ may be defined by a reducible degree-4 polynomial and hence may violate the Hasse principle; thus the conclusion $\mu(\mathcal{W}(k)) = \mathbb{A}^1(k)$ in Proposition 6.2 must be weakened to $\mu(\mathcal{W}(k)) \subseteq \mathbb{A}^1(k)$, and this eventually implies $\pi_c(Y_c(k)) \subseteq U(k)$.

On the other hand, an argument of Parshin (see [Szp85]) shows that Faltings' proof of the Mordell conjecture can be adapted to give an upper bound on the *size* of each set $C_i'(k)$ in the proof of Lemma 6.1. Therefore we can compute a bound on $\#T$. Choose a finite subset $\Gamma \subseteq k^\times$ whose image in $k^\times/k^{\times 2}$ is disjoint from the image of F and has size greater than $\#T$. Then Γ contains at least one good c.

Let $Y = \coprod_{c \in \Gamma} Y_c$, and define $\pi\colon Y \to X$ by $\pi|_{Y_c} = \pi_c$. Then $\pi(Y(k)) = \bigcup_{c\in\Gamma} \pi_c(Y_c(k)) = U(k)$ since all terms in the union are subsets of $U(k)$ and some term equals $U(k)$. □

9. Algorithms for rational points

Proof of Theorem 1.1(i). Suppose we want to know whether the k-variety U has a k-point. By passing to a finite open cover, we may assume that U is affine. Let X be a projective closure of U. Construct $Y \to X$ be as in Theorem 1.3. Let $Y_1, \ldots, Y_n$ be the connected components of Y. If Y_i is geometrically integral, by assumption we can decide whether Y_i has a k-point. If Y_i is not geometrically integral, then since Y_i is regular, it has no k-point. Thus we can decide whether Y has a k-point, and the answer for U is the same. □

Proof of Theorem 1.1(ii). We want to compute $\#X(k)$. Apply the algorithm of Theorem 1.1(i) to X. If it says that X has no k-point, we are done. Otherwise, search until a k-point P on X is found, and start over with the variety $X - \{P\}$. If $X(k)$ is finite, this algorithm will eventually terminate. (This kind of argument was used also in [Kim03].) □

10. Global function fields

In this section, we investigate whether the proofs of the previous sections carry over to the case where k is a global function field of characteristic not 2.

The main issues are

(1) The two-part paper [CTSSD87, CTSSD87b], which is key to all our main results, works only over number fields. But it seems likely that the same proofs work, with at most minor modifications, over any global field of characteristic not 2.
(2) The proof of Theorem 1.3 uses resolution of singularities, which is not proved in positive characteristic. Moreover, the proof of Theorem 1.1 uses Theorem 1.3 so it also is in question. Without assuming resolution of singularities, one would obtain the weaker versions of Theorem 1.1 and 1.3 in which the word "regular" is removed from both.

There are a few other issues, but these can be circumvented, as we now discuss.

The proof of Proposition 4.1 works for any global function field k of characteristic not 2: fix a place ∞ of k, let $\mathcal{O}_k$ be the ring of functions that are regular outside ∞, and replace the archimedean and 2-adic conditions on a and b by the condition that a and b be squares in the completion k_∞; then the proof proceeds as before.

The second paragraph of the proof of Lemma 6.1 encounters two problems in positive characteristic: first, it needs ν_i to be separable, and second, to apply the function field analogue [Sam66] of Faltings' theorem it needs C'_i to be non-isotrivial. As for the first problem, if in Section 5 we choose $\tilde{P}_\infty(w,x)$ to be separable, then the same will be true of $\tilde{P}_\infty + v^2\tilde{P}_0$ over $k(v)$, and the same will be true of the ν_i in the application of Lemma 6.1, since the ν_i correspond to field extensions of $k(v)$ contained in the splitting field of $\tilde{P}_\infty + v^2\tilde{P}_0$ over $k(v)$. As for the second problem, the flexibility in the choice of Q in the proof of Lemma 6.1 lets us arrange for C'_i to be non-isotrivial. Moreover, in this case, one can bound not only the number of k-points on each C'_i, but also their height [Szp81, §8, Corollaire 2].

There is another thing that is better over global function fields k than over number fields. Namely, by a proved generalization of Hilbert's tenth problem to such k [Phe91, Shl92, Vid94, Eis03], it is already known that there is no algorithm for deciding whether a k-variety has a k-point. Therefore, if k is a global function field of characteristic not 2, and we assume that [CTSSD87, CTSSD87b] works over k, then there is no algorithm for deciding whether a projective geometrically integral k-variety has a k-point (and if we moreover assume resolution of singularities, we can add the adjective "regular" in this final statement).

11. Open questions

(i) Can one generalize Remark 1.2(f) to show that to have algorithms in (i) and (ii) of Theorem 1.1 for n-folds, it would suffice to be able to decide the existence of rational points on regular projective geometrically integral $(n+2)$-*folds*.
(ii) Is there a proof of Proposition 4.1 that does not require such explicit calculations?
(iii) Is the problem of deciding whether a smooth projective geometrically integral *hypersurface* over k has a k-point also equivalent to the problem for arbitrary k-varieties?

Acknowledgements

I thank Jean-Louis Colliot-Thélène for several helpful comments, Brian Conrad for encouraging me to examine the function field analogue, Thomas Graber for a remark leading to Proposition 6.3, and J. Felipe Voloch and Olivier Wittenberg for suggesting some references.

References

[CT98] J.-L. Colliot-Thélène, *The Hasse principle in a pencil of algebraic varieties*, Number theory (Tiruchirapalli, 1996), Contemp. Math., vol. 210, Amer. Math. Soc., Providence, RI, 1998, pp. 19–39. MR **1478483 (98g:**11075) ↑5

[CTCS80] Jean-Louis Colliot-Thélène, Daniel Coray, and Jean-Jacques Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*, J. Reine Angew. Math. **320** (1980), 150–191 (French). MR **592151 (82f:**14020) ↑1.2, 4

[CTP00] Jean-Louis Colliot-Thélène and Bjorn Poonen, *Algebraic families of nonzero elements of Shafarevich-Tate groups*, J. Amer. Math. Soc. **13** (2000), no. 1, 83–99.MR1697093 (2000f:11067) ↑5, 6

[CTSSD87a] Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, and Peter Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. I*, J. Reine Angew. Math. **373** (1987), 37–107. MR **870307 (88m:**11045a) ↑4, 5, 6, 1, 10

[CTSSD87b] ———, *Intersections of two quadrics and Châtelet surfaces. II*, J. Reine Angew. Math. **374** (1987), 72–168. MR **876222 (88m:**11045b) ↑4, 1, 10

[Eis03] Kirsten Eisenträger, *Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific J. Math. **210** (2003), no. 2, 261–281. MR **1988534 (2004d:**12014) ↑10

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German); English transl., *Finiteness theorems for abelian varieties over number fields* (1986), 9–27. Erratum in: Invent. Math. **75** (1984), 381.MR718935 (85g:11026a) ↑6

[Isk71] V. A. Iskovskikh, *A counterexample to the Hasse principle for systems of two quadratic forms in five variables*, Mat. Zametki **10** (1971), 253–257 (Russian). MR 0286743 (44 #3952) ↑4

[Kim03] Minhyong Kim, *Relating decision and search algorithms for rational points on curves of higher genus*, Arch. Math. Logic **42** (2003), no. 6, 563–568. MR **2001059 (2004f:**14039) ↑1.2, 9

[Lan54] Serge Lang, *Some applications of the local uniformization theorem*, Amer. J. Math. **76** (1954), 362–374. MR 0062722 (16,7a) ↑1.2

[Nis55] Hajime Nishimura, *Some remarks on rational points*, Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math. **29** (1955), 189–192. MR 0095851 (20 #2349) ↑1.2

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), no. 1, 1–8. MR **1079837 (92e:**11145) ↑10

[Sam66] Pierre Samuel, *Compléments à un article de Hans Grauert sur la conjecture de Mordell*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 29, 55–62 (French).MR0204430 (34 #4272) ↑10

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre.MR1757192 (2000m:11049) ↑5.1, 5

[Shl92] Alexandra Shlapentokh, *Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic*, Trans. Amer. Math. Soc. **333** (1992), no. 1, 275–298. MR **1091233 (92m:**11144) ↑10

[Sko01] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001.MR1845760 (2002d:14032) ↑4

[Smo91] Craig Smoryński, *Logical number theory. I*, Universitext, Springer-Verlag, Berlin, 1991. An introduction. MR **1106853 (92g:**03001) ↑1.2

[Szp81] Lucien Szpiro, *Propriétés numériques du faisceau dualisant relatif*, Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux, Astérisque, vol. 86, Société Mathématique de France, 1981, pp. 44–78 (French). MR **642675 (83c:**14020) ↑10

[Szp85] ———, *Un peu d'effectivité*, Astérisque (1985), no. 127, 275–287 (French). Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). MR 801928 ↑8

[Vid94] Carlos R. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), no. 1, 249–253. MR **1159179 (94b:**11122) ↑10

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: `poonen@math.berkeley.edu`
URL: `http://math.berkeley.edu/~poonen/`